

BIPARTITE EULER SYSTEMS

BENJAMIN HOWARD

ABSTRACT. If E is an elliptic curve over \mathbf{Q} and K is an imaginary quadratic field, there is an Iwasawa main conjecture predicting the behavior of the Selmer group of E over the anticyclotomic \mathbf{Z}_p -extension of K . The main conjecture takes different forms depending on the sign of the functional equation of $L(E/K, s)$. In the present work we combine ideas of Bertolini and Darmon with those of Mazur and Rubin to show that the main conjecture, regardless of the sign of the functional equation, can be reduced to proving the nonvanishing of sufficiently many p -adic L -functions attached to a family of congruent modular forms.

1. INTRODUCTION

Let E be an elliptic curve over \mathbf{Q} with conductor N , and let K be a quadratic imaginary field of discriminant d_K prime to N with quadratic character ϵ . By work of Gross and Zagier, the sign of the functional equation of $L(E/K, s)$ is equal to $-\epsilon(N)$. For a rational prime $p \nmid 6d_K N$ at which E has good *ordinary* reduction, let D_∞/K be the anticyclotomic \mathbf{Z}_p -extension of K . The behavior of the Selmer group $\text{Sel}_{p^\infty}(E/D_\infty)$ depends crucially on the value of $\epsilon(N)$: if $\epsilon(N) = 1$ then it is conjectured that the Pontryagin dual, X , of $\text{Sel}_{p^\infty}(E/D_\infty)$ has rank one over the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\text{Gal}(D_\infty)/K]]$ and that the characteristic ideal of the torsion submodule can be expressed in terms of Heegner points arising from a Shimura curve parametrization of E . We call this the indefinite case. In the definite case, $\epsilon(N) = -1$, it is conjectured that X is a torsion Λ -module with characteristic ideal given by a p -adic L -function. We refer to these two conjectures collectively as the Iwasawa main conjecture.

Much is known about the Iwasawa main conjecture, see [1, 8, 9] for the indefinite case and [2] for the definite case. In particular, in either case one knows that the rank of X is as predicted above, and one knows one divisibility of the conjectured equality for the characteristic ideal of the torsion submodule (in the indefinite case this is conditional on as yet unpublished work of Cornut and Vatsal generalizing the main result of [4] to Heegner points on Shimura curves attached to indefinite quaternion algebras, see the main results of [9]). The goal of the present article is to demonstrate that the methods used by Bertolini and Darmon [2] to treat the definite case can be used give a uniform treatment of the two cases, and to develop a criterion to determine when the known divisibility is actually an equality. We do this by developing a theory of *bipartite Euler systems* similar in spirit to Mazur and Rubin's [10] theory of Kolyvagin systems, but adapted to fit the family of cohomology classes constructed by Bertolini and Darmon.

Date: February 29, 2012.

2000 *Mathematics Subject Classification.* 11G05, 11G40, 11R23.

This research was supported by an NSF postdoctoral fellowship.

Bertolini and Darmon's construction is, roughly speaking, as follows. Let f be the modular form of level N attached to E . For a choice of positive integer k one can define a set of *admissible* primes \mathfrak{L}_k , all of which are inert in K , with the property that for any $n \in \mathfrak{N}_k$ (the set of squarefree products of primes in \mathfrak{L}_k) there is a modular form f_n of level nN which is congruent to f modulo p^k . This modular form comes to us via a generalization of Ribet's well-known level raising theorem. Define a graph whose vertices are the elements of \mathfrak{N}_k with edges connecting n to $n\ell$ for each coprime $n \in \mathfrak{N}_k$ and $\ell \in \mathfrak{L}_k$. A vertex n is said to be either definite or indefinite depending on whether $\epsilon(nN)$ is -1 or 1 , respectively, and this defines a bipartition of the graph: every edge connects a definite vertex to an indefinite vertex. At an indefinite vertex the modular form f_n allows one to define a cohomology class $\kappa_n \in \varprojlim_r H^1(D_r/K, E[p^k])$, which arises as the Kummer image of Heegner points on the abelian variety attached to f_n . At a definite vertex one can attach to f_n a p -adic L -function $\lambda_n \in \Lambda/p^k\Lambda$. There are reciprocity laws relating the elements at any two adjacent vertices; these reciprocity laws are examples of Jochowitz congruences in the sense of [3]. The *pair* of families

$$\{\kappa_n \mid n \in \mathfrak{N}_k, n \text{ indefinite}\} \quad \{\lambda_n \mid n \in \mathfrak{N}_k, n \text{ definite}\}$$

is then our prototype of a bipartite Euler system. Our main result asserts that the existence of a bipartite Euler system implies one divisibility of the Iwasawa main conjecture, and if one can prove sufficiently many nonvanishing theorems for the p -adic L -functions λ_n then equality holds in the Iwasawa main conjecture. To emphasize, this approach treats the definite and indefinite cases on completely equal footing. The precise statement is given in Theorem 3.2.3.

The reader is referred to [2] for the details of the construction sketched above. In the present article we simply assume that a pair of families satisfying the appropriate axioms is given. It should be noted that Bertolini and Darmon do not construct enough classes to provide an Euler system in our sense. Those authors assume that $\epsilon(N) = -1$ and that f is p -isolated [2, Definition 1.2], and then choose a particular path (starting at the vertex corresponding to the empty product 1) in the graph defined above. The Euler system elements are then constructed *only at vertices along that path*. The path is not allowed to be arbitrary: it is required that the modular form f_n is again p -isolated at each definite vertex in the path. It would thus be necessary to remove the p -isolated hypothesis in order to make full use of the theory developed herein.

Recently Darmon and Iovita [5] have adapted the methods of [2] to the case where $\epsilon(N) = -1$ and p is a prime of *supersingular* reduction for E . Given the results of the present article, it seems likely that these ideas can be pushed further to cover all four cases (definite/ordinary, indefinite/ordinary, definite/supersingular, and indefinite/supersingular; the final case being the least well understood). The main (only?) obstruction to doing so is the removal of the technical p -isolated hypothesis referred to above.

We remark that the idea that Euler systems can be used not only to bound Selmer groups, but also to give a criterion for the sharpness of the bound, goes back to Kolyvagin. This was extended to the Iwasawa-theoretic setting by Mazur and Rubin [10], but the criterion for equality seems very difficult to verify in practice. In the usual theory of Euler systems, in e.g. [12], one begins with cohomology classes (related in some way to L -functions) defined over abelian extensions of the ground field K , and then applies Kolyvagin's derivative operators to these classes to

obtain classes defined over K itself. These derived classes are the *Kolyvagin system*, and are somewhat less directly related to L -functions than the Euler system from which they are derived. The criterion for equality (e.g. the *primitivity* of [10] Definitions 4.5.5 and 5.3.9) is then a nonvanishing statement for the Kolyvagin system, rather than for the Euler system itself. The observation that Bertolini and Darmon's methods make no use of Kolyvagin's derivative operators is what allows us to obtain a criterion for equality in the main conjecture directly in terms of (p -adic) L -functions.

Finally, and somewhat more speculatively, we address the question of whether there exist bipartite Euler systems other than that constructed by Bertolini and Darmon. Gross and Kudla [7] have investigated the Rankin triple product L -function $L(f \times g \times h, s)$ associated to three newforms f, g, h of weight 2 on $\Gamma_0(N)$. This L -function has analytic continuation and functional equation in $s \mapsto 4 - s$, and the sign in the functional equation is given by a simple formula. When this sign is 1, Gross and Kudla prove a special value formula similar to Gross's special value formula [6] in the Heegner point situation, a key ingredient in the reciprocity laws used in [2]. When the sign in the functional equation is -1 , Gross and Kudla construct a special homologically trivial cycle in the codimension 1 Chow group of a triple product of Shimura curves. Applying the p -adic Abel-Jacobi map to this special cycle yields a class in the Galois cohomology of the tensor product $V_f \otimes V_g \otimes V_h$ of the p -adic Galois representations attached to f, g, h . Thus we have the beginnings of a bipartite Euler system for $V_f \otimes V_g \otimes V_h$. Moreover, Gross and Kudla conjecture that the height of their special cycle in the Chow group is related to the derivative $L'(f \times g \times h, 2)$, in close analogy with the Gross-Zagier formula.

2. EULER SYSTEMS OVER ARTINIAN RINGS

In this section we develop a general theory of (bipartite) Euler systems. The axioms (Definition 2.3.2) are designed to include the family of cohomology classes used by Bertolini and Darmon [2]. The methods used to bound the associated Selmer group and to develop a criterion for equality (Theorems 2.3.7 and 2.5.1) originated with Kolyvagin, and we follow closely the approach to Kolyvagin's theory described by Mazur and Rubin [10].

Let R be a principal Artinian local ring with maximal ideal \mathfrak{m} and residue characteristic $p > 3$. Let T be a free R -module of rank two equipped with a continuous (for the discrete topology) action of $G_K \stackrel{\text{def}}{=} \text{Gal}(K^{\text{alg}}/K)$ for some number field K . We assume that T admits a perfect, G_K -equivariant, alternating $R(1)$ -valued pairing. Let

$$\text{loc}_w : H^1(K, T) \rightarrow H^1(K_w, T)$$

denote the localization map (we assume that we are given a fixed embedding $K^{\text{alg}} \hookrightarrow K_w^{\text{alg}}$ for every place w). Throughout §2 we assume that we are given a fixed self-dual Selmer structure $(\mathcal{F}, \Sigma_{\mathcal{F}})$ on T , as defined in §2.1.

If B is any R -module and $b \in B$ we define $\text{ind}(b, B)$, the *index of divisibility* of b in B , to be the largest $k \leq \infty$ such that $b \in \mathfrak{m}^k B$.

2.1. Selmer modules.

Definition 2.1.1. A *Selmer structure* $(\mathcal{F}, \Sigma_{\mathcal{F}})$ on T is a finite set of places $\Sigma_{\mathcal{F}}$ of K containing the archimedean places, the primes at which T is ramified, and the

prime p ; and, for every place w of K , a choice of submodule

$$H_{\mathcal{F}}^1(K_w, T) \subset H^1(K_w, T)$$

such that $H_{\mathcal{F}}^1(K_w, T) = H_{\text{unr}}^1(K_w, T)$ for all $w \notin \Sigma_{\mathcal{F}}$. Define the *Selmer module* $\text{Sel}_{\mathcal{F}} = \text{Sel}_{\mathcal{F}}(K, T)$ associated to \mathcal{F} by the exactness of

$$0 \rightarrow \text{Sel}_{\mathcal{F}} \rightarrow H^1(K, T) \xrightarrow{\oplus \text{loc}_w} \bigoplus_w H^1(K_w, T) / H_{\mathcal{F}}^1(K_w, T)$$

where the sum is over all places w of K . A Selmer structure \mathcal{F} is *self-dual* if the submodule $H_{\mathcal{F}}^1(K_w, T)$ is maximal isotropic under the (symmetric) local Tate pairing

$$H^1(K_w, T) \times H^1(K_w, T) \xrightarrow{\cup} H^2(K_w, R(1)) \cong R$$

for every finite place $w \in \Sigma_{\mathcal{F}}$.

Remark 2.1.2. Note that $p \neq 2$ implies $H^1(K_w, T) = 0$ for w archimedean. By Tate local duality, $H_{\mathcal{F}}^1(K_w, T) = H_{\text{unr}}^1(K_w, T)$ is maximal isotropic for all $w \notin \Sigma_{\mathcal{F}}$.

Remark 2.1.3. If S is a submodule (resp. quotient) of T and $(\mathcal{F}, \Sigma_{\mathcal{F}})$ is a Selmer structure on T , then there is an induced Selmer structure, still denoted $(\mathcal{F}, \Sigma_{\mathcal{F}})$, on S defined as the preimage of $H_{\mathcal{F}}^1(K_w, T)$ under $H^1(K_w, S) \rightarrow H^1(K_w, T)$ (resp. the image of $H_{\mathcal{F}}^1(K_w, T)$ under $H^1(K_w, T) \rightarrow H^1(K_w, S)$) for every place w of K . By [10, Lemma 1.1.9], $H_{\mathcal{F}}^1(K_w, S) = H_{\text{unr}}^1(K_w, S)$ for every $w \notin \Sigma_{\mathcal{F}}$, and so this is well-defined. We refer to this as *propagation* of Selmer structures.

2.2. Modified Selmer modules. Now suppose we have a set of primes \mathfrak{L} of K which is disjoint from $\Sigma_{\mathcal{F}}$ and satisfies

- (a) $\forall \mathfrak{l} \in \mathfrak{L}, \mathbf{N}(\mathfrak{l}) \not\equiv 1 \pmod{p}$,
- (b) $\forall \mathfrak{l} \in \mathfrak{L}$, the Frobenius $\text{Frob}_{\mathfrak{l}}$ acts on T with eigenvalues $\mathbf{N}(\mathfrak{l})$ and 1.

Let \mathfrak{N} denote the set of squarefree products of primes in \mathfrak{L} . The two conditions above imply that $T \cong R \oplus R(1)$ as a $\text{Gal}(K_{\mathfrak{l}}^{\text{alg}}/K_{\mathfrak{l}})$ -module, and that the decomposition is unique. For each $\mathfrak{l} \in \mathfrak{L}$ we define the *ordinary* cohomology $H_{\text{ord}}^1(K_{\mathfrak{l}}, T)$ to be the image of $H^1(K_{\mathfrak{l}}, R(1)) \rightarrow H^1(K_{\mathfrak{l}}, T)$.

Lemma 2.2.1. *For $\mathfrak{l} \in \mathfrak{L}$, the decomposition $T \cong R \oplus R(1)$ induces a decomposition*

$$H^1(K_{\mathfrak{l}}, T) \cong H_{\text{unr}}^1(K_{\mathfrak{l}}, T) \oplus H_{\text{ord}}^1(K_{\mathfrak{l}}, T)$$

in which each summand is free of rank one over R and is maximal isotropic under the local Tate pairing.

Proof. By [12, Lemma 1.3.2], evaluation of cocycles at $\text{Frob}_{\mathfrak{l}}$ induces an isomorphism

$$H_{\text{unr}}^1(K_{\mathfrak{l}}, T) \cong T / (\text{Frob}_{\mathfrak{l}} - 1)T \cong R.$$

By local class field theory

$$H^1(K_{\mathfrak{l}}, R) \cong \text{Hom}(\text{Gal}(K_{\mathfrak{l}}^{\text{unr}}/K_{\mathfrak{l}}), R) \cong R,$$

again by evaluation at $\text{Frob}_{\mathfrak{l}}$. Thus $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ is exactly the image of $H^1(K_{\mathfrak{l}}, R)$, and is free of rank one. Since $\mathbf{N}(\mathfrak{l}) \not\equiv 1 \pmod{p}$, the pro- p -completion of $K_{\mathfrak{l}}^{\times}$ is canonically isomorphic to \mathbf{Z}_p , and so

$$H_{\text{ord}}^1(K_{\mathfrak{l}}, T) \cong H^1(K_{\mathfrak{l}}, R(1)) \cong R$$

by local Kummer theory. The submodules R and $R(1)$ of T are each maximal isotropic under the pairing $T \times T \rightarrow R(1)$, and so the same is true of the spaces $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ and $H_{\text{ord}}^1(K_{\mathfrak{l}}, T)$ under the cup product. \square

Definition 2.2.2. A Selmer structure $(\mathcal{F}, \Sigma_{\mathcal{F}})$ is *cartesian* if for every quotient $T/\mathfrak{m}^i T$ of T , every place $w \in \Sigma_{\mathcal{F}}$, and any generator $\pi \in \mathfrak{m}$, the isomorphism

$$T/\mathfrak{m}^i T \xrightarrow{\pi^{\text{length}(R)-i}} T[\mathfrak{m}^i]$$

induces an isomorphism $H_{\mathcal{F}}^1(K_w, T/\mathfrak{m}^i) \cong H_{\mathcal{F}}^1(K_w, T[\mathfrak{m}^i])$.

Remark 2.2.3. A Selmer structure $(\mathcal{F}, \Sigma_{\mathcal{F}})$ is cartesian if and only if it defines a cartesian local condition, for every $w \in \Sigma_{\mathcal{F}}$, on the quotient category $\text{Quot}(T)$ in the sense of [10, Definition 1.1.4].

Hypothesis 2.2.4. For the remainder of §2 we make the following assumptions

- (a) the residual representation $T/\mathfrak{m}T$ is absolutely irreducible,
- (b) \mathcal{F} is cartesian.

Definition 2.2.5. For any $\mathfrak{abc} \in \mathfrak{N}$ we define a Selmer structure $(\mathcal{F}_{\mathfrak{b}}^{\mathfrak{a}}(\mathfrak{c}), \Sigma_{\mathcal{F}_{\mathfrak{b}}^{\mathfrak{a}}(\mathfrak{c})})$ as follows: $\Sigma_{\mathcal{F}_{\mathfrak{b}}^{\mathfrak{a}}(\mathfrak{c})}$ is $\Sigma_{\mathcal{F}}$ together with all prime divisors of \mathfrak{abc} ,

$$H_{\mathcal{F}_{\mathfrak{b}}^{\mathfrak{a}}(\mathfrak{c})}^1(K_w, T) = H_{\mathcal{F}}^1(K_w, T)$$

for w prime to \mathfrak{abc} , and

$$H_{\mathcal{F}_{\mathfrak{b}}^{\mathfrak{a}}(\mathfrak{c})}^1(K_{\mathfrak{l}}, T) = \begin{cases} H^1(K_{\mathfrak{l}}, T) & \text{if } \mathfrak{l} \nmid \mathfrak{a} \\ 0 & \text{if } \mathfrak{l} \nmid \mathfrak{b} \\ H_{\text{ord}}^1(K_{\mathfrak{l}}, T) & \text{if } \mathfrak{l} \nmid \mathfrak{c}. \end{cases}$$

If any one of \mathfrak{a} , \mathfrak{b} , \mathfrak{c} is the empty product we omit it from the notation.

Lemma 2.2.6. *The Selmer structure $\mathcal{F}(\mathfrak{n})$ is cartesian for any $\mathfrak{n} \in \mathfrak{N}$. For any choice of generator $\pi \in \mathfrak{m}$ and any $0 \leq i \leq \text{length}(R)$, the composition*

$$T/\mathfrak{m}^i T \xrightarrow{\pi^{\text{length}(R)-i}} T[\mathfrak{m}^i] \rightarrow T$$

induces isomorphisms

$$\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}^i) \cong \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T[\mathfrak{m}^i]) \cong \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}^i].$$

Proof. For any prime w not dividing \mathfrak{n} , $H_{\mathcal{F}(\mathfrak{n})}^1(K_w, T)$ satisfies the cartesian property by Hypothesis 2.2.4. For $\mathfrak{l} \nmid \mathfrak{n}$, the cartesian property follows from the canonical isomorphism $H_{\text{ord}}^1(K_{\mathfrak{l}}, T) \cong R$ used in the proof of Lemma 2.2.1. The second claim now follows as in [10, Lemma 3.5.4]. \square

Proposition 2.2.7. *For any $\mathfrak{n} \in \mathfrak{N}$ there is a (non-canonical) decomposition*

$$\text{Sel}_{\mathcal{F}(\mathfrak{n})} \cong R^{e(\mathfrak{n})} \oplus M_{\mathfrak{n}} \oplus M_{\mathfrak{n}}$$

with $e(\mathfrak{n}) \in \{0, 1\}$.

Proof. This follows from the existence of a modified form of the Cassels-Tate pairing, together with the self-duality hypotheses on T and \mathcal{F} ; see [8, Theorem 1.4.2]. \square

Definition 2.2.8. Let $\mathfrak{N}^{\text{even}} \subset \mathfrak{N}$ be the subset for which $e(\mathfrak{n}) = 0$, and $\mathfrak{N}^{\text{odd}} \subset \mathfrak{N}$ the subset for which $e(\mathfrak{n}) = 1$. For $\mathfrak{n} \in \mathfrak{N}$ we define the *stub module*

$$\text{Stub}_{\mathfrak{n}} = \begin{cases} \mathfrak{m}^{\text{length}(M_{\mathfrak{n}})} \cdot R & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}} \\ \mathfrak{m}^{\text{length}(M_{\mathfrak{n}})} \cdot \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T) & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}} \end{cases}$$

with $M_{\mathfrak{n}}$ as in Proposition 2.2.7. Note that $\text{Stub}_{\mathfrak{n}}$ is a cyclic R -module for every $\mathfrak{n} \in \mathfrak{N}$.

The following proposition is a consequence of Poitou-Tate global duality, and is similar to [8, Lemma 1.5.8] and [10, Lemma 4.1.6]. Our self-duality assumptions, together with the fact that the local conditions $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ and $H_{\text{ord}}^1(K_{\mathfrak{l}}, T)$ have rank one, give a much stronger result.

Proposition 2.2.9. *For any $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}$ there are non-negative integers a, b with $a+b = \text{length}(R)$ such that in the diagram of inclusions*

$$\begin{array}{ccc} & \text{Sel}_{\mathcal{F}^{\mathfrak{l}}(\mathfrak{n})} & \\ \nearrow b & & \nwarrow a \\ \text{Sel}_{\mathcal{F}(\mathfrak{n})} & & \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})} \\ \nwarrow a & & \nearrow b \\ & \text{Sel}_{\mathcal{F}_{\mathfrak{l}}(\mathfrak{n})} & \end{array}$$

the labels on the arrows are the lengths of the respective quotients. All four quotients are cyclic R -modules and

$$(1) \quad a = \text{length}(\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n})})) \quad b = \text{length}(\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})).$$

Proof. Take (1) as the definition of a and b , so that a and b are the lengths of the lower left and right quotients, respectively. The cyclicity of the quotients follows from Lemma 2.2.1; for example the lower left quotient injects into $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$.

Exactly as in the proof of [8, Lemma 1.5.7], the quotient

$$(2) \quad \text{Sel}_{\mathcal{F}^{\mathfrak{l}}(\mathfrak{n})} / (\text{Sel}_{\mathcal{F}(\mathfrak{n})} + \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})$$

admits a nondegenerate, alternating R -valued pairing. The pairing is defined as follows: given $x, y \in \text{Sel}_{\mathcal{F}^{\mathfrak{l}}(\mathfrak{n})}$, let x' be the projection of $\text{loc}_{\mathfrak{l}}(x)$ to $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$, and let y' be the projection of $\text{loc}_{\mathfrak{l}}(y)$ to $H_{\text{ord}}^1(K_{\mathfrak{l}}, T)$. The pairing of x and y is then defined to be the local Tate pairing of x' and y' . The quotient (2) is a cyclic R -module, and so the existence of such a pairing implies that it is trivial.

Directly from the definitions we have

$$\text{Sel}_{\mathcal{F}_{\mathfrak{l}}(\mathfrak{n})} = \text{Sel}_{\mathcal{F}(\mathfrak{n})} \cap \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}.$$

Combining this with the above, it follows that the lower left quotient is isomorphic to the upper right, and the lower right is isomorphic to the upper left. This proves everything except for the claim $a+b = \text{length}(R)$, which is a consequence of global duality as in [8, Lemma 1.5.8] or [10, Lemma 4.1.6]. \square

Corollary 2.2.10. *Fix $\mathfrak{n} \in \mathfrak{N}$ and let $e(\mathfrak{n})$ be as in Proposition 2.2.7. The integer*

$$\rho(\mathfrak{n}) = \dim_{R/\mathfrak{m}}(\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T))$$

satisfies $e(\mathfrak{n}) \equiv \rho(\mathfrak{n}) \pmod{2}$, and for any $\mathfrak{l} \in \mathfrak{L}$ prime to \mathfrak{n}

$$\begin{aligned} \rho(\mathfrak{n}\mathfrak{l}) &= \rho(\mathfrak{n}) + 1 && \iff \text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T)) = 0 \\ \rho(\mathfrak{n}\mathfrak{l}) &= \rho(\mathfrak{n}) - 1 && \iff \text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T)) \neq 0. \end{aligned}$$

The claim continues to hold, and the value of $\rho(\mathfrak{n})$ remains unchanged, if one replaces $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T)$ by $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}]$ everywhere.

Proof. Apply Proposition 2.2.9 with T replaced by $T/\mathfrak{m}T$. Then

$$\rho(\mathfrak{n}\mathfrak{l}) = \rho(\mathfrak{n}) - a + b,$$

$a + b = 1$, and $a = 0$ if and only if $\text{loc}_{\mathfrak{l}}$ kills $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T)$. Combining this with Lemma 2.2.6 proves the claim. \square

Remark 2.2.11. Note that Corollary 2.2.10 implies that for $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}$,

$$\mathfrak{n} \in \mathfrak{N}^{\text{even}} \iff \mathfrak{n}\mathfrak{l} \in \mathfrak{N}^{\text{odd}}.$$

We will use this repeatedly throughout.

Corollary 2.2.12. *Suppose $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}$, and let a and b be as in Proposition 2.2.9. Then*

$$\text{length}(M_{\mathfrak{n}}) = \begin{cases} \text{length}(M_{\mathfrak{n}\mathfrak{l}}) + a & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}} \\ \text{length}(M_{\mathfrak{n}\mathfrak{l}}) - b & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}}. \end{cases}$$

Proof. Suppose $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$. Then

$$\begin{aligned} 2 \cdot \text{length}(M_{\mathfrak{n}}) &= \text{length}(\text{Sel}_{\mathcal{F}(\mathfrak{n})}) \\ &= \text{length}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}) - b + a \\ &= \text{length}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}) + 2a - \text{length}(R) \\ &= 2 \cdot \text{length}(M_{\mathfrak{n}\mathfrak{l}}) + 2a. \end{aligned}$$

The case $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$ is similar. \square

Corollary 2.2.13. *Suppose $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}$. There is an isomorphism of R -modules*

$$\begin{aligned} \text{loc}_{\mathfrak{l}}(\text{Stub}_{\mathfrak{n}}) &\cong \text{Stub}_{\mathfrak{n}\mathfrak{l}} && \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}} \\ \text{loc}_{\mathfrak{l}}(\text{Stub}_{\mathfrak{n}\mathfrak{l}}) &\cong \text{Stub}_{\mathfrak{n}} && \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}}. \end{aligned}$$

Proof. Suppose $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$. Since the modules in question are cyclic, it suffices to check that they have the same annihilator in R . The image of $\text{Stub}_{\mathfrak{n}}$ in $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ is annihilated by \mathfrak{m}^i if and only if $\mathfrak{m}^{i+\text{length}(M_{\mathfrak{n}})}$ kills the lower left quotient in the diagram of Proposition 2.2.9, that is, if and only if $a \leq i + \text{length}(M_{\mathfrak{n}})$. By Corollary 2.2.12, this is equivalent to $\text{length}(R) \leq i + \text{length}(M_{\mathfrak{n}\mathfrak{l}})$, which is equivalent to $\mathfrak{m}^i \cdot \text{Stub}_{\mathfrak{n}\mathfrak{l}} = 0$. The case $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$ is similar. \square

2.3. Euler systems. Continue to assume that Hypothesis 2.2.4 holds, as well as

Hypothesis 2.3.1. For any $c \in H^1(K, T/\mathfrak{m}T)$ there are infinitely many $\mathfrak{l} \in \mathfrak{L}$ such that $\text{loc}_{\mathfrak{l}}(c) \neq 0$.

Definition 2.3.2. A *bipartite Euler system of odd type* for $(T, \mathcal{F}, \mathfrak{L})$ is a pair of families

$$\{\kappa_{\mathfrak{n}} \in \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T) \mid \mathfrak{n} \in \mathfrak{N}^{\text{odd}}\} \quad \{\lambda_{\mathfrak{n}} \in R \mid \mathfrak{n} \in \mathfrak{N}^{\text{even}}\}$$

related by the first and second reciprocity laws:

(a) for any $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}^{\text{odd}}$, there exists an isomorphism of R -modules

$$R/(\lambda_{\mathfrak{n}}) \cong H_{\text{ord}}^1(K_{\mathfrak{l}}, T)/R \cdot \text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}),$$

(b) for any $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}^{\text{even}}$, there exists an isomorphism of R -modules

$$R/(\lambda_{\mathfrak{n}\mathfrak{l}}) \cong H_{\text{unr}}^1(K_{\mathfrak{l}}, T)/R \cdot \text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}}).$$

A *bipartite Euler system of even type* is defined in the same way, but with even and odd interchanged everywhere in the definition.

From here on we drop the adjective “bipartite”, and simply call such a pair of families an Euler system. An Euler system (of even or odd type) is *nontrivial* if $\lambda_{\mathfrak{n}} \neq 0$ for some \mathfrak{n} (of the appropriate type). By the reciprocity laws and the following lemma, this is equivalent to $\kappa_{\mathfrak{n}} \neq 0$ for some \mathfrak{n} of the appropriate type.

Lemma 2.3.3. *For any $\mathfrak{n} \in \mathfrak{N}$ and any cyclic R -submodule $C \subset \text{Sel}_{\mathcal{F}(\mathfrak{n})}$, there are infinitely many $\mathfrak{l} \in \mathfrak{L}$ such that $\text{loc}_{\mathfrak{l}}$ takes C injectively into $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$. If C is free of rank one then for such any such \mathfrak{l} , $\text{loc}_{\mathfrak{l}}$ takes C isomorphically onto $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$.*

Proof. Let i be maximal such that $\mathfrak{m}^i C \neq 0$, so that $\mathfrak{m}^i C \subset \text{Sel}_{\mathcal{F}(\mathfrak{n})}[\mathfrak{m}]$. By Hypothesis 2.3.1 and Lemma 2.2.6, there are infinitely many $\mathfrak{l} \in \mathfrak{L}$ prime to \mathfrak{n} such that $\text{loc}_{\mathfrak{l}}(\mathfrak{m}^i C) \neq 0$. For any such prime $\text{loc}_{\mathfrak{l}}$ takes C injectively into $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$. The final claim is immediate from Lemma 2.2.1. \square

Proposition 2.3.4. *There are no nontrivial Euler systems for $(T, \mathcal{F}, \mathfrak{L})$ of even type.*

Proof. Given a nontrivial Euler system of even type we fix $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$ such that $\lambda_{\mathfrak{n}} \neq 0$. In the notation of Proposition 2.2.7, $e(\mathfrak{n}) = 1$, and so $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T)$ contains a free rank-one R -submodule C . If $\mathfrak{l} \in \mathfrak{L}$ is chosen as in Lemma 2.3.3 then the natural injection

$$\text{Sel}_{\mathcal{F}(\mathfrak{n})}/\text{Sel}_{\mathcal{F}_{\mathfrak{l}}(\mathfrak{n})} \hookrightarrow H_{\text{unr}}^1(K_{\mathfrak{l}}, T) \cong R$$

is an isomorphism, and Proposition 2.2.9 implies that $\text{Sel}_{\mathcal{F}_{\mathfrak{l}}(\mathfrak{n})} = \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}$. In particular $\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}) = 0$, violating the first reciprocity law. \square

Proposition 2.3.5. *Fix an Euler system of odd type for $(T, \mathcal{F}, \mathfrak{L})$, let k be the length of R , and let $M_{\mathfrak{n}}$ be as in Proposition 2.2.7. If $\lambda_{\mathfrak{n}} \neq 0$ for some $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$ then $M_{\mathfrak{n}}$ is killed by \mathfrak{m}^{k-1} . If $\kappa_{\mathfrak{n}} \neq 0$ for some $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$ then $M_{\mathfrak{n}}$ is killed by \mathfrak{m}^{k-1} .*

Proof. First suppose $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$ and $\mathfrak{m}^{k-1} M_{\mathfrak{n}} \neq 0$. Then $\text{Sel}_{\mathcal{F}(\mathfrak{n})}$ contains a free rank one submodule, C . Choose $\mathfrak{l} \in \mathfrak{L}$ not dividing \mathfrak{n} such that $\text{loc}_{\mathfrak{l}}$ takes C isomorphically onto $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ (Lemma 2.3.3). By Proposition 2.2.9, $\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}) = 0$. Thus $\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}) = 0$ and the first reciprocity law implies that $\lambda_{\mathfrak{n}} = 0$.

Now suppose $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$ and $\mathfrak{m}^{k-1} M_{\mathfrak{n}} \neq 0$. Proposition 2.2.7 implies that $\text{Sel}_{\mathcal{F}(\mathfrak{n})}$ contains a free submodule of rank two, C . From this and Lemma 2.2.1 one may deduce that for any $\mathfrak{l} \in \mathfrak{L}$ the kernel of

$$\text{loc}_{\mathfrak{l}} : \text{Sel}_{\mathcal{F}(\mathfrak{n})} \rightarrow H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$$

contains a free submodule. This kernel is exactly $\text{Sel}_{\mathcal{F}_{\mathfrak{l}}(\mathfrak{n})} \subset \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}$, and so $\mathfrak{m}^{k-1} M_{\mathfrak{n}\mathfrak{l}} \neq 0$. By the case considered above $\lambda_{\mathfrak{n}\mathfrak{l}} = 0$, and the second reciprocity law implies that $\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}}) = 0$. Since this holds for all choices of \mathfrak{l} , $\kappa_{\mathfrak{n}} = 0$ by Lemma 2.3.3. \square

The above proposition shows that an Euler system gives a (somewhat weak) annihilation result for Selmer groups. To strengthen this to an upper bound on Selmer groups, we must impose the hypothesis of *freeness* defined below. For an example of how this hypothesis may be verified in practice, see the proof of Lemma 3.3.6.

Definition 2.3.6. We will say that an Euler system of odd type is *free* if for every $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$, there is a free rank-one R -submodule $C_{\mathfrak{n}} \subset \text{Sel}_{\mathcal{F}(\mathfrak{n})}$ containing $\kappa_{\mathfrak{n}}$.

Theorem 2.3.7. *For any free Euler system of odd type for $(T, \mathcal{F}, \mathfrak{L})$, $\lambda_{\mathfrak{n}} \in \text{Stub}_{\mathfrak{n}}$ for every $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$, and $\kappa_{\mathfrak{n}} \in \text{Stub}_{\mathfrak{n}}$ for every $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$. Equivalently, the R -module $M_{\mathfrak{n}}$ of Proposition 2.2.7 satisfies*

$$\text{length}(M_{\mathfrak{n}}) \leq \begin{cases} \text{ind}(\lambda_{\mathfrak{n}}, R) & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}} \\ \text{ind}(\kappa_{\mathfrak{n}}, \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T)) & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}}. \end{cases}$$

Proof. The proof is by induction on $\rho(\mathfrak{n})$, as defined in Corollary 2.2.10. If $\rho(\mathfrak{n}) = 0$ then $M_{\mathfrak{n}} = 0$, and so $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$, $\text{Stub}_{\mathfrak{n}} = R$, and the claim is vacuous. Similarly, if $\rho(\mathfrak{n}) = 1$ then $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$, $M_{\mathfrak{n}} = 0$, and the claim is vacuous. We assume now that $\rho(\mathfrak{n}) \geq 2$, so that $M_{\mathfrak{n}} \neq 0$.

Suppose $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$ and $\lambda_{\mathfrak{n}} \neq 0$. Fix any $\mathfrak{l} \in \mathfrak{L}$ prime to \mathfrak{n} such that the Selmer group $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}T)$ is not killed by $\text{loc}_{\mathfrak{l}}$. By Corollary 2.2.10 and the induction hypothesis, $\kappa_{\mathfrak{n}\mathfrak{l}} \in \text{Stub}_{\mathfrak{n}\mathfrak{l}}$, and so Corollary 2.2.12 gives

$$\begin{aligned} \text{length}(M_{\mathfrak{n}}) &= \text{length}(M_{\mathfrak{n}\mathfrak{l}}) + a \\ &\leq \text{ind}(\kappa_{\mathfrak{n}\mathfrak{l}}, \text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})}) + a \\ &\leq \text{ind}(\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}), \text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})) + a \end{aligned}$$

where a is as in Proposition 2.2.9. The first reciprocity law implies

$$\begin{aligned} \text{ind}(\lambda_{\mathfrak{n}}, R) &= \text{ind}(\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}), H_{\text{ord}}^1(K_{\mathfrak{l}}, T)) \\ &= \text{ind}(\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}), \text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})) + \text{length}(H_{\text{ord}}^1(K_{\mathfrak{l}}, T)/\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})) \\ &= \text{ind}(\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}}), \text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathfrak{n}\mathfrak{l})})) + \text{length}(R) - b. \end{aligned}$$

Since $a + b = \text{length}(R)$, we conclude $\text{length}(M_{\mathfrak{n}}) \leq \text{ind}(\lambda_{\mathfrak{n}}, R)$.

Now suppose $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$ and $\kappa_{\mathfrak{n}} \neq 0$. Let $C_{\mathfrak{n}}$ be as in Definition 2.3.6 and fix $\mathfrak{l} \in \mathfrak{L}$ prime to \mathfrak{n} such that $\text{loc}_{\mathfrak{l}}$ takes $C_{\mathfrak{n}}$ isomorphically onto $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$ (using Lemma 2.3.3). Again applying Corollary 2.2.10, $\rho(\mathfrak{n}\mathfrak{l}) = \rho(\mathfrak{n}) - 1$, and so $\lambda_{\mathfrak{n}\mathfrak{l}} \in \text{Stub}_{\mathfrak{n}\mathfrak{l}}$. By Corollary 2.2.12 (with $a = \text{length}(R)$ and $b = 0$) and the second reciprocity law,

$$\begin{aligned} \text{length}(M_{\mathfrak{n}}) = \text{length}(M_{\mathfrak{n}\mathfrak{l}}) &\leq \text{ind}(\lambda_{\mathfrak{n}\mathfrak{l}}, R) \\ &= \text{ind}(\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}}), H_{\text{unr}}^1(K_{\mathfrak{l}}, T)) \\ &= \text{ind}(\kappa_{\mathfrak{n}}, \text{Sel}_{\mathcal{F}(\mathfrak{n})}). \end{aligned}$$

□

2.4. Sheaves on graphs. Let \mathcal{X} be the graph whose vertices $v(\mathfrak{n})$ are indexed by $\mathfrak{n} \in \mathfrak{N}$, and an edge $e(\mathfrak{n}, \mathfrak{n}\mathfrak{l})$ connects $v(\mathfrak{n})$ to $v(\mathfrak{n}\mathfrak{l})$ whenever $\mathfrak{l} \in \mathfrak{L}$ and $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}$. A vertex $v(\mathfrak{n})$ will be called even or odd, depending on whether \mathfrak{n} lies in $\mathfrak{N}^{\text{even}}$ or $\mathfrak{N}^{\text{odd}}$, and every edge connects an even vertex to an odd one (by Corollary 2.2.10).

We define a sheaf $\text{ES}(\mathcal{X})$ on \mathcal{X} in the sense of [10, §3.1] called the *Euler system sheaf* as follows. To each vertex $v = v(\mathbf{n})$ we attach the R -module

$$\text{ES}(v) = \begin{cases} \text{Sel}_{\mathcal{F}(\mathbf{n})} & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{odd}} \\ R & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{even}} \end{cases}$$

and to each edge $e = e(\mathbf{n}, \mathbf{n}\mathfrak{l})$ we attach the R -module

$$\text{ES}(e) = \begin{cases} H_{\text{unr}}^1(K_{\mathfrak{l}}, T) & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{odd}} \\ H_{\text{ord}}^1(K_{\mathfrak{l}}, T) & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{even}}. \end{cases}$$

If $e = e(\mathbf{n}, \mathbf{n}\mathfrak{l})$ is an edge with endpoint v , we define the *vertex-to-edge map*

$$\psi_v^e : \text{ES}(v) \rightarrow \text{ES}(e)$$

as follows. If v is odd then

$$\psi_v^e = \text{loc}_{\mathfrak{l}} : \begin{cases} \text{Sel}_{\mathcal{F}(\mathbf{n})} \rightarrow H_{\text{unr}}^1(K_{\mathfrak{l}}, T) & \text{if } v = v(\mathbf{n}) \\ \text{Sel}_{\mathcal{F}(\mathbf{n}\mathfrak{l})} \rightarrow H_{\text{ord}}^1(K_{\mathfrak{l}}, T) & \text{if } v = v(\mathbf{n}\mathfrak{l}). \end{cases}$$

If v is even then fix, using Lemma 2.2.1, an isomorphism

$$(3) \quad \psi_v^e : R \cong \begin{cases} H_{\text{unr}}^1(K_{\mathfrak{l}}, T) & \text{if } v = v(\mathbf{n}\mathfrak{l}) \\ H_{\text{ord}}^1(K_{\mathfrak{l}}, T) & \text{if } v = v(\mathbf{n}). \end{cases}$$

Of course, the choice of isomorphism (3) is not unique, but we fix a choice, for each edge e with even vertex v , once and for all.

Definition 2.4.1. The Euler system sheaf has a locally cyclic (in the sense of [10, Definition 3.4.2]) subsheaf, the *stub sheaf* $\text{Stub}(\mathcal{X})$, defined as follows. To each vertex $v = v(\mathbf{n})$ we attach the cyclic R -module

$$\text{Stub}(v) = \text{Stub}_{\mathbf{n}} \subset \text{ES}(v),$$

and to each edge $e = e(\mathbf{n}, \mathbf{n}\mathfrak{l})$ we attach the cyclic module $\text{Stub}(e) \subset \text{ES}(e)$

$$\text{Stub}(e) = \begin{cases} \text{loc}_{\mathfrak{l}}(\text{Stub}_{\mathbf{n}}) & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{odd}} \\ \text{loc}_{\mathfrak{l}}(\text{Stub}_{\mathbf{n}\mathfrak{l}}) & \text{if } \mathbf{n} \in \mathfrak{N}^{\text{even}}. \end{cases}$$

If e is an edge connecting the vertices v and v' , with v even and v' odd, then the vertex-to-edge map $\psi_{v'}^e$ restricts to a surjective map $\text{Stub}(v') \rightarrow \text{Stub}(e)$. By Corollary 2.2.13, the map ψ_v^e restricts to an isomorphism $\text{Stub}(v) \cong \text{Stub}(e)$.

Definition 2.4.2. A *core vertex* of \mathcal{X} is a vertex v such that $\text{Stub}(v) \cong R$.

Remark 2.4.3. Set $\overline{T} = T/\mathfrak{m}T$. For $\mathbf{n} \in \mathfrak{N}$, recall the integer

$$\rho(\mathbf{n}) = \dim_{R/\mathfrak{m}}(\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T}))$$

of Corollary 2.2.10. It is clear from Lemma 2.2.6 and Proposition 2.2.7 that $v(\mathbf{n})$ is a core vertex if and only if $\rho(\mathbf{n}) = 0$ or 1.

The *core subgraph* $\mathcal{X}_0 \subset \mathcal{X}$ is the graph whose vertices are the core vertices of \mathcal{X} , with two vertices connected by an edge in \mathcal{X}_0 if and only if they are connected by an edge in \mathcal{X} . We let $\text{Stub}(\mathcal{X}_0)$ be the restriction of $\text{Stub}(\mathcal{X})$ to \mathcal{X}_0 in the obvious sense.

Lemma 2.4.4. *The sheaf $\text{Stub}(\mathcal{X}_0)$ is locally free of rank one. That is to say,*

- *for every vertex v of \mathcal{X}_0 , $\text{Stub}(v)$ is free of rank one,*
- *for every edge e of \mathcal{X}_0 , $\text{Stub}(e)$ is free of rank one,*

- for every edge e of \mathcal{X}_0 with endpoint v , the vertex-to-edge map

$$\psi_v^e : \text{Stub}(v) \rightarrow \text{Stub}(e)$$

is an isomorphism.

Proof. The first property is the definition of \mathcal{X}_0 . As noted in Definition 2.4.1, $\text{Stub}(e)$ is isomorphic to $\text{Stub}(v)$, where v is the even endpoint of e . This proves the second property. The final property follows from the first two, together with the surjectivity of the vertex-to-edge maps in $\text{Stub}(\mathcal{X})$. \square

Definition 2.4.5. A *global section*, s , of the sheaf $\text{Stub}(\mathcal{X})$ on \mathcal{X} is a function on vertices and edges of \mathcal{X} ,

$$v \mapsto s(v) \in \text{Stub}(v) \quad e \mapsto s(e) \in \text{Stub}(e),$$

such that for every edge e with endpoints v and v'

$$\psi_v^e(s(v)) = s(e) = \psi_{v'}^e(s(v'))$$

in $\text{Stub}(e)$. A global section of $\text{ES}(\mathcal{X})$ is defined in the same way.

Definition 2.4.6. For two vertices v and v' of \mathcal{X} , a *path* from v to v' in \mathcal{X} is a finite sequence of vertices $v = v_0, v_1, \dots, v_k = v'$ such that v_i is connected to v_{i+1} by an edge e_i . A path is *surjective* (for the locally cyclic sheaf $\text{Stub}(\mathcal{X})$) if the vertex-to-edge map

$$\psi_{v_{i+1}}^{e_i} : \text{Stub}(v_{i+1}) \rightarrow \text{Stub}(e_i)$$

is an isomorphism for every i . We make the same definitions for \mathcal{X}_0 .

Remark 2.4.7. Note that a surjective path from v to v' induces in an obvious way ([10, §3.4]) a surjective map $\text{Stub}(v) \rightarrow \text{Stub}(v')$, and that for any global section s of $\text{Stub}(\mathcal{X})$ this map takes $s(v)$ to $s(v')$.

Lemma 2.4.8. A path v_0, \dots, v_k in \mathcal{X} is surjective if and only if

$$\text{length}(\text{Stub}(v_{i+1})) \leq \text{length}(\text{Stub}(v_i))$$

for every i .

Proof. Suppose we are given a path in \mathcal{X} from v_0 to v_k . If v_i is odd and v_{i+1} is even then the vertex-to-edge map $\text{Stub}(v_{i+1}) \rightarrow \text{Stub}(e_i)$ is an isomorphism, while $\text{Stub}(v_i) \rightarrow \text{Stub}(e_i)$ is surjective. Thus the path v_i, v_{i+1} is surjective and $\text{length}(\text{Stub}(v_{i+1})) \leq \text{length}(\text{Stub}(v_i))$.

If v_i is even and v_{i+1} is odd then the vertex-to-edge map $\text{Stub}(v_{i+1}) \rightarrow \text{Stub}(e_i)$ is surjective, while $\text{Stub}(v_i) \rightarrow \text{Stub}(e_i)$ is an isomorphism. In particular

$$\text{length}(\text{Stub}(v_{i+1})) \geq \text{length}(\text{Stub}(v_i)).$$

Thus $\psi_{v_{i+1}}^{e_i}$ is injective if and only if it is an isomorphism. This is equivalent to $\text{Stub}(v_{i+1}) \cong \text{Stub}(v_i)$, which is equivalent to

$$\text{length}(\text{Stub}(v_{i+1})) \leq \text{length}(\text{Stub}(v_i)).$$

Since v_0, \dots, v_k is surjective if and only if v_i, v_{i+1} is a surjective path for every i , the claim follows. \square

Lemma 2.4.9. For any vertex v of \mathcal{X} there is a core vertex v_0 and a surjective path in \mathcal{X} from v_0 to v . For any $\mathfrak{n} \in \mathfrak{N}$ there is a $\mathfrak{n}' \in \mathfrak{N}$ with $\mathfrak{n}|\mathfrak{n}'$ such that $v(\mathfrak{n}')$ is a core vertex, and \mathfrak{n}' may be chosen either in $\mathfrak{N}^{\text{even}}$ or in $\mathfrak{N}^{\text{odd}}$.

Proof. Set $w_0 = v$, and construct a sequence of vertices w_i inductively as follows.

If $w_i = w(\mathbf{n}_i)$ is even and not a core vertex, choose $\mathfrak{l} \in \mathfrak{L}$ prime to \mathbf{n}_i such that $\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathbf{n}_i)}) \neq 0$, and set $w_{i+1} = w(\mathbf{n}_i \mathfrak{l})$. In the notation of Corollary 2.2.12, $a > 0$, and so

$$\text{length}(\text{Stub}(w_i)) < \text{length}(\text{Stub}(w_{i+1})).$$

If w_i is already an even core vertex, then a similar argument shows that

$$\text{length}(\text{Stub}(w_i)) = \text{length}(\text{Stub}(w_{i+1}))$$

for any choice of \mathfrak{l} .

If $w_i = w(\mathbf{n}_i)$ is odd choose (using Lemma 2.3.3) $\mathfrak{l} \in \mathfrak{L}$ prime to \mathbf{n}_i such that localization at \mathfrak{l} takes a free rank-one submodule of $\text{Sel}_{\mathcal{F}(\mathbf{n}_i)}$ isomorphically onto $H_{\text{unr}}^1(K_{\mathfrak{l}}, T)$, and set $w_{i+1} = w(\mathbf{n}_i \mathfrak{l})$. In the notation of Corollary 2.2.12, $a = \text{length}(R)$ and $b = 0$, and so

$$\text{length}(\text{Stub}(w_i)) = \text{length}(\text{Stub}(w_{i+1})).$$

Eventually $\text{length}(\text{Stub}(w_k)) = \text{length}(R)$, and we have constructed a path from v to a core vertex $v_0 = w_k$. By construction

$$\text{length}(\text{Stub}(w_i)) \leq \text{length}(\text{Stub}(w_{i+1}))$$

for every i , and so Lemma 2.4.8 implies that the path w_k, w_{k-1}, \dots, w_0 is a surjective path from v_0 to v . The final claim is clear from the construction above. \square

For any $\mathfrak{a} \in \mathfrak{N}$, let $\mathcal{X}_{0,\mathfrak{a}}$ be the subgraph of \mathcal{X}_0 whose vertices consist of those core vertices $v(\mathbf{n})$ with $\mathfrak{a}|\mathbf{n}$. Two vertices are connected by an edge in $\mathcal{X}_{0,\mathfrak{a}}$ if and only if they are connected by an edge in \mathcal{X}_0 .

Lemma 2.4.10. *If $v(\mathfrak{a})$ is a core vertex then the graph $\mathcal{X}_{0,\mathfrak{a}}$ is path connected.*

Proof. Fix $\mathbf{n} = \mathfrak{a}\mathfrak{b} \in \mathfrak{N}$. We show by induction on the number of prime factors of \mathfrak{b} that there is a path in $\mathcal{X}_{0,\mathfrak{a}}$ from $v(\mathbf{n})$ to $v(\mathfrak{a})$. Assume $\mathfrak{b} > 1$, otherwise there is nothing to prove. First suppose $v(\mathbf{n})$ is even, so that $\rho(\mathbf{n}) = 0$. By Corollary 2.2.10, $\rho(\mathbf{n}/\mathfrak{l}) = 1$ for any $\mathfrak{l} \in \mathfrak{L}$ dividing \mathfrak{b} . Hence $v(\mathbf{n}/\mathfrak{l})$ is a vertex in $\mathcal{X}_{0,\mathfrak{a}}$ connected to $v(\mathbf{n})$ by an edge, and by the induction hypothesis there is a path in $\mathcal{X}_{0,\mathfrak{a}}$ from $v(\mathbf{n}/\mathfrak{l})$ to $v(\mathfrak{a})$. Similarly, if $v(\mathbf{n})$ is odd and $\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T})) \neq 0$ for some \mathfrak{l} dividing \mathfrak{b} , then Proposition 2.2.9 implies $\rho(\mathbf{n}/\mathfrak{l}) = \rho(\mathbf{n}) - 1 = 0$, and again by we are done by the induction hypothesis.

We are left to treat the case where $\mathbf{n} \in \mathfrak{N}^{\text{even}}$ and $\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T}))$ is trivial for every \mathfrak{l} dividing \mathfrak{b} . Thus

$$\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T}) = \text{Sel}_{\mathcal{F}_{\mathfrak{b}}(\mathfrak{a})}(K, \overline{T}) \subset \text{Sel}_{\mathcal{F}(\mathfrak{a})}(K, \overline{T}).$$

Since the R/\mathfrak{m} -vector space on the left has dimension $\rho(\mathbf{n}) = 1$ while the space on the right has dimension $\rho(\mathfrak{a}) \leq 1$, we conclude that the above inclusion is an equality. In particular

$$\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T}) = \text{Sel}_{\mathcal{F}_{\mathfrak{b}'}(\mathfrak{a})}(K, \overline{T}) = \text{Sel}_{\mathcal{F}(\mathfrak{a})}(K, \overline{T})$$

for any $\mathfrak{b}'|\mathfrak{b}$. Take $\mathfrak{b}' = \mathfrak{b}/\mathfrak{q}$ for some prime \mathfrak{q} dividing \mathfrak{b} , and let $\mathfrak{l} \in \mathfrak{L}$ be any prime not dividing \mathbf{n} such that $\text{loc}_{\mathfrak{l}}(\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T})) \neq 0$. By Corollary 2.2.10, $\rho(\mathfrak{a}\mathfrak{b}') = 2$, $\rho(\mathbf{n}\mathfrak{l}) = 0$, and, since

$$\text{Sel}_{\mathcal{F}(\mathbf{n})}(K, \overline{T}) = \text{Sel}_{\mathcal{F}_{\mathfrak{b}}(\mathfrak{a})}(K, \overline{T}) \subset \text{Sel}_{\mathcal{F}(\mathfrak{a}\mathfrak{b}')} (K, \overline{T})$$

is not killed by loc_l , $\rho(\mathfrak{ab}'l) = 1$. Thus $v(\mathfrak{ab}), v(\mathfrak{abl}), v(\mathfrak{ab}'l)$ is a path in $\mathcal{X}_{0,\mathfrak{a}}$. Finally, if $\text{loc}_r(\text{Sel}_{\mathcal{F}(\mathfrak{ab}'l)}(K, \overline{T})) = 0$ for every $\mathfrak{r} \in \mathfrak{L}$ dividing $\mathfrak{b}'l$, then

$$\text{Sel}_{\mathcal{F}(\mathfrak{ab}'l)}(K, \overline{T}) = \text{Sel}_{\mathcal{F}_{\mathfrak{b}'l}(\mathfrak{a})}(K, \overline{T}) \subset \text{Sel}_{\mathcal{F}_{\mathfrak{b}'}(\mathfrak{a})}(K, \overline{T}) = \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, \overline{T}).$$

The Selmer groups on the left and right are both one dimensional over R/\mathfrak{m} , so equality holds everywhere. This contradicts $\text{loc}_l(\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, \overline{T})) \neq 0$, and we conclude that $\text{loc}_r(\text{Sel}_{\mathcal{F}(\mathfrak{ab}'l)}(K, \overline{T})) \neq 0$ for some $\mathfrak{r} \in \mathfrak{L}$ dividing $\mathfrak{b}'l$. This returns us to the case of the paragraph above, and so $v(\mathfrak{n}), v(\mathfrak{n}l), v(\mathfrak{ab}'l), v(\mathfrak{ab}'l/\mathfrak{r})$ is a path in \mathcal{X}_0 . By the induction hypothesis, this may be continued to a path terminating at $v(\mathfrak{a})$. \square

Proposition 2.4.11. *The core subgraph is path connected and contains both even and odd vertices. For any vertex v of \mathcal{X} and any core vertex v_0 of \mathcal{X} , there is a surjective path from v_0 to v .*

Proof. The fact that \mathcal{X}_0 contains both even and odd vertices follows from the final statement of Lemma 2.4.9. Suppose we are given two core vertices $v(\mathfrak{a})$ and $v(\mathfrak{b})$. By the second part of Lemma 2.4.9 we may choose $\mathfrak{n} \in \mathfrak{N}$ divisible by \mathfrak{ab} such that $v(\mathfrak{n})$ is a core vertex. By Lemma 2.4.10, there is a path in $\mathcal{X}_{0,\mathfrak{a}}$ from $v(\mathfrak{a})$ to $v(\mathfrak{n})$, and a path in $\mathcal{X}_{0,\mathfrak{b}}$ from $v(\mathfrak{b})$ to $v(\mathfrak{n})$. Since any path in $\mathcal{X}_{0,\mathfrak{a}}$ is also a path in \mathcal{X}_0 , and similarly for \mathfrak{b} , there is a path in \mathcal{X}_0 from $v(\mathfrak{a})$ to $v(\mathfrak{b})$. Since any path in \mathcal{X}_0 is surjective, any two core vertices may be connected by a surjective path. The final claim now follows from Lemma 2.4.9. \square

Corollary 2.4.12. *For any global section s of $\text{Stub}(\mathcal{X})$ there is a unique $\delta = \delta(s)$ with $0 \leq \delta \leq \text{length}(R)$ such that $s(v)$ generates $\mathfrak{m}^\delta \text{Stub}(v)$ for every vertex v of \mathcal{X} . The section s is determined by its value at any core vertex.*

Proof. Fix a core vertex v_0 and define δ to be such that $s(v_0)$ generates $\mathfrak{m}^\delta \text{Stub}(v_0)$. By Remark 2.4.7 and Proposition 2.4.11, for any vertex v in \mathcal{X} there is a surjective map $\text{Stub}(v_0) \rightarrow \text{Stub}(v)$ taking $s(v_0)$ to $s(v)$. The claim follows. \square

2.5. The rigidity theorem.

Theorem 2.5.1. *Assume Hypotheses 2.2.4 and 2.3.1, and suppose that we are given a nontrivial free Euler system of odd type for $(T, \mathcal{F}, \mathfrak{L})$. There is a unique integer δ , independent of $\mathfrak{n} \in \mathfrak{N}$, with the property that $\lambda_{\mathfrak{n}}$ generates $\mathfrak{m}^\delta \text{Stub}_{\mathfrak{n}}$ for every $\mathfrak{n} \in \mathfrak{N}^{\text{even}}$ and $\kappa_{\mathfrak{n}}$ generates $\mathfrak{m}^\delta \text{Stub}_{\mathfrak{n}}$ for every $\mathfrak{n} \in \mathfrak{N}^{\text{odd}}$. Furthermore, δ is given by*

$$\begin{aligned} \delta &= \min\{\text{ind}(\lambda_{\mathfrak{n}}, R) \mid \mathfrak{n} \in \mathfrak{N}^{\text{even}}\} \\ &= \min\{\text{ind}(\kappa_{\mathfrak{n}}, \text{Sel}_{\mathcal{F}(\mathfrak{n})}) \mid \mathfrak{n} \in \mathfrak{N}^{\text{odd}}\}. \end{aligned}$$

Proof. For a vertex $v = v(\mathfrak{n})$ of the graph \mathcal{X} of §2.4, we define $s(v) \in \text{ES}(v)$ by

$$s(v) = \begin{cases} \lambda_{\mathfrak{n}} & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}} \\ \kappa_{\mathfrak{n}} & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}}. \end{cases}$$

For an edge $e = e(\mathfrak{n}, \mathfrak{n}l)$ define $s(e) \in \text{ES}(e)$ by

$$s(e) = \begin{cases} \text{loc}_l(\kappa_{\mathfrak{n}}) & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{odd}} \\ \text{loc}_l(\kappa_{\mathfrak{n}l}) & \text{if } \mathfrak{n} \in \mathfrak{N}^{\text{even}}. \end{cases}$$

The reciprocity laws of Definition 2.3.2 now say exactly that, modifying the vertex-to-edge maps (3) by an element of R^\times if needed, the function $v \mapsto s(v)$ forms a

global section of the Euler system sheaf $\text{ES}(\mathcal{X})$ with edge germ $e \mapsto s(e)$. By Theorem 2.3.7, this global section is actually a global section of the subsheaf $\text{Stub}(\mathcal{X}) \subset \text{ES}(\mathcal{X})$. By Corollary 2.4.12, there is a unique $0 \leq \delta < \text{length}(R)$ such that $s(v)$ generates $\mathfrak{m}^\delta \cdot \text{Stub}(v)$ for every vertex v . For any vertex v with $s(v) \neq 0$ we have

$$\delta = \text{ind}(s(v), \text{Stub}(v)) \leq \text{ind}(s(v), \text{ES}(v))$$

with equality if and only if v is a core vertex. Since there are even core vertices (by Proposition 2.4.11),

$$\delta = \min\{ \text{ind}(s(v), \text{ES}(v)) \mid v \text{ even} \},$$

and similarly with even replaced by odd. \square

2.6. A variant. In the applications to Iwasawa theory we will need to work under slightly different hypothesis on T . In this subsection we assume that K is a quadratic imaginary field. Fix an embedding $K^{\text{alg}} \hookrightarrow \mathbb{C}$ and let $\tau \in G_K$ be the associated complex conjugation. Let R and T be as in the introduction to §2, but instead of assuming that T is self Cartier dual via an alternating pairing, assume, as in §1.3 of [8], that there is a perfect *symmetric* pairing

$$(\ , \) : T \times T \rightarrow R(1)$$

which satisfies $(x^\sigma, y^{\tau\sigma\tau}) = (x, y)^\sigma$ for any $\sigma \in G_K$. Let $\text{Tw}(T)$ be the G_K -module whose underlying R -module is T , but with the G_K -action twisted by conjugation by τ . The above pairing can then be viewed as a perfect G_K -invariant pairing

$$T \times \text{Tw}(T) \rightarrow R(1).$$

There is a canonical isomorphism $H^1(K, T) \cong H^1(K, \text{Tw}(T))$ given on cocycles by $c(\sigma) \mapsto c^*(\sigma) = c(\tau\sigma\tau)$. For any finite place v of K , there is similarly a canonical isomorphism from the local cohomology of T at v to the local cohomology of $\text{Tw}(T)$ at $\tau(v)$. This isomorphism induces a local Tate pairing

$$(4) \quad H^1(K_v, T) \times H^1(K_{\tau(v)}, T) \rightarrow R,$$

and by direct calculation on cocycles one can check that if $v = \tau(v)$ then this pairing is symmetric. Thus locally at a degree two prime of K , the cohomology of T behaves exactly as if T were self-dual via an alternating pairing. We now define a Selmer structure $(\mathcal{F}, \Sigma_{\mathcal{F}})$ exactly as in §2.1, and say that a Selmer structure is self-dual if the local conditions $H_{\mathcal{F}}^1(K_v, T)$ and $H_{\mathcal{F}}^1(K_{\tau(v)}, T)$ are exact orthogonal complements under the pairing (4) for every $v \in \Sigma_{\mathcal{F}}$.

All of the results of §2 hold verbatim under these modified hypothesis (one need only verify that Lemma 2.2.1 and Propositions 2.2.7 and 2.2.9 hold, as these are the only places where the self-duality hypotheses on T and \mathcal{F} are directly invoked; for the latter two, the reader may consult Sections 1.4 and 1.5 of [8]) with one minor caveat: the statement of Lemma 2.2.1 and the proof of Proposition 2.2.9 require the self-duality of $H^1(K_I, T)$, and so we must add the hypothesis that \mathfrak{L} contains only degree two primes of K .

Finally, we remark that if the action of G_K on T extends to an action of $G_{\mathbf{Q}}$ then the alternate hypotheses of this subsection are equivalent to those of the introduction to §2, since one may identify $T \cong \text{Tw}(T)$ as G_K -modules via the map $x \mapsto x^\tau$.

3. IWASAWA THEORY OF ELLIPTIC CURVES

Let K be a quadratic imaginary field of discriminant d_K and quadratic character ϵ , $p > 3$ a rational prime, and E/\mathbf{Q} an elliptic curve with conductor N . Assume that E has either multiplicative or good ordinary reduction at p , and that $(d_K, pN) = 1$. Let N^- be the largest divisor of N which is prime to p and satisfies $\epsilon(q) = 1$ for all primes $q \mid N^-$. Factor $N = N^+ N^-$. Let τ be a fixed choice of complex conjugation.

Hypothesis 3.0.1. Throughout §3 we assume:

- (a) $E[p]$ is absolutely irreducible as a $G_K = \text{Gal}(K^{\text{alg}}/K)$ -module,
- (b) N^- is squarefree.

We denote by D_∞ the anticyclotomic \mathbf{Z}_p -extension of K , characterized by $\tau\sigma\tau = \sigma^{-1}$ for any $\sigma \in \Gamma = \text{Gal}(D_\infty/K)$. Let $D_m \subset D_\infty$ be the subfield with $[D_m : K] = p^m$, and set $\Lambda = \mathbf{Z}_p[[\Gamma]]$.

3.1. Selmer modules over Λ .

Definition 3.1.1. A degree two prime $\mathfrak{l} \nmid N$ of K is *k-admissible* if $\mathbf{N}(\mathfrak{l}) \not\equiv 1 \pmod{p}$, and if there is a decomposition

$$E[p^k] \cong (\mathbf{Z}/p^k\mathbf{Z}) \oplus \mu_{p^k}$$

of $\text{Gal}(K_{\mathfrak{l}}^{\text{unr}}/K_{\mathfrak{l}})$ -modules. A 1-admissible prime will simply be called *admissible*. The set of *k*-admissible primes is denoted \mathfrak{L}_k , and we let \mathfrak{N}_k denote the set of squarefree products of primes in \mathfrak{L}_k .

Let $q \mid N^-$ be a rational prime. By Hypothesis 3.0.1(b) E has multiplicative reduction at q , and hence split multiplicative reduction at the prime \mathfrak{q} of K above q . The Tate parametrization shows that $T_p(E)$ has the form $\begin{pmatrix} \epsilon_{\text{cyc}} & * \\ 0 & 1 \end{pmatrix}$ as a $G_{K_{\mathfrak{q}}}$ -module, and we denote by $\text{Fil}_q(T_p(E)) \subset T_p(E)$ the \mathbf{Z}_p -line on which $G_{K_{\mathfrak{q}}}$ acts via ϵ_{cyc} . For any extension $L/K_{\mathfrak{q}}$ the *ordinary* submodule

$$H_{\text{ord}}^1(L, T_p(E)) \subset H^1(L, T_p(E))$$

is defined to be the image of $H^1(L, \text{Fil}_q(T_p(E)))$, and $H_{\text{ord}}^1(L, E[p^k])$ is defined similarly. For a *k*-admissible prime $\mathfrak{l} \in \mathfrak{L}_k$ we have a similar ordinary local condition $H_{\text{ord}}^1(L, E[p^k])$ for any extension $L/K_{\mathfrak{l}}$, as in §2.2. For the prime p , $T_p(E)$ has a distinguished line on which an inertia group at p in $G_{\mathbf{Q}}$ acts via the cyclotomic character. Call this line $\text{Fil}_p(T_p(E))$ and define the ordinary condition at p to be the image of

$$H^1(L, \text{Fil}_p(T_p(E))) \rightarrow H^1(L, T_p(E))$$

for any finite extension L/\mathbf{Q}_p , and similarly for $E[p^k]$ and $E[p^\infty]$.

Lemma 3.1.2. For any $\mathfrak{l} \in \mathfrak{L}_k$ the module

$$\varprojlim_m H_{\text{unr}}^1(D_{m, \mathfrak{l}}, E[p^k]) \stackrel{\text{def}}{=} \varprojlim_m \bigoplus_{w \mid \mathfrak{l}} H_{\text{unr}}^1(D_{m, w}, E[p^k])$$

is free of rank one over $\Lambda/p^k\Lambda$, and the same is true with *unr* replaced by *ord*.

Proof. Since \mathfrak{l} splits completely in D_∞ , Shapiro's lemma gives an isomorphism

$$\varprojlim_m \bigoplus_{w \mid \mathfrak{l}} H^1(D_{m, w}, E[p^k]) \cong H^1(K_{\mathfrak{l}}, E[p^k] \otimes \Lambda) \cong H^1(K_{\mathfrak{l}}, E[p^k]) \otimes \Lambda.$$

This, together with Lemma 2.2.1, gives the claim. \square

We define the Selmer groups

$$\mathcal{S}(D_\infty, T_p(E)) \subset \varprojlim H^1(D_m, T_p(E)) \quad \text{Sel}(D_\infty, E[p^\infty]) \subset \varprojlim H^1(D_m, E[p^\infty])$$

to be the classes which are ordinary at the primes dividing pN^- and unramified at all other primes, and abbreviate

$$\mathcal{S} = \mathcal{S}(D_\infty, T_p(E)) \quad X = \text{Hom}(\text{Sel}(D_\infty, E[p^\infty]), \mathbf{Q}_p/\mathbf{Z}_p).$$

For any $\mathfrak{n} \in \mathfrak{N}_k$, let

$$\mathcal{S}_{\mathfrak{n}}(D_\infty, E[p^k]) \subset \varprojlim_m H^1(D_m, E[p^k])$$

be the Λ -submodule of classes which are ordinary at the primes dividing $\mathfrak{n}pN^-$, and unramified at all other primes.

3.2. Euler systems over Λ .

Definition 3.2.1. Given $\mathfrak{n} \in \mathfrak{N}_1$, let n be the positive integer satisfying $n\mathcal{O}_K = \mathfrak{n}$. We say that \mathfrak{n} is *definite* if $\epsilon(nN^-) = -1$, and is *indefinite* if $\epsilon(nN^-) = 1$. Let $\mathfrak{N}_k^{\text{definite}} \subset \mathfrak{N}_k$ be the subset of definite products, and define $\mathfrak{N}_k^{\text{indefinite}}$ similarly.

Suppose that for every $k > 0$ we are given families

$$(5) \quad \{\kappa_{\mathfrak{n}} \in \mathcal{S}_{\mathfrak{n}}(D_\infty, E[p^k]) \mid \mathfrak{n} \in \mathfrak{N}_k^{\text{indefinite}}\} \quad \{\lambda_{\mathfrak{n}} \in \Lambda/p^k\Lambda \mid \mathfrak{n} \in \mathfrak{N}_k^{\text{definite}}\}$$

which, as k varies, are compatible with the inclusion $\mathfrak{N}_{k+1} \subset \mathfrak{N}_k$ and the natural maps $\Lambda/p^{k+1}\Lambda \rightarrow \Lambda/p^k\Lambda$ and $E[p^{k+1}] \xrightarrow{p} E[p^k]$. Assume that these classes satisfy the first and second reciprocity laws:

- (a) for any $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}_k^{\text{indefinite}}$ there is an isomorphism of Λ -modules

$$\varprojlim_m H_{\text{ord}}^1(D_{m,\mathfrak{l}}, E[p^k]) \cong \Lambda/p^k\Lambda$$

taking $\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}\mathfrak{l}})$ to $\lambda_{\mathfrak{n}}$;

- (b) for any $\mathfrak{n}\mathfrak{l} \in \mathfrak{N}_k^{\text{definite}}$ there is an isomorphism of Λ -modules

$$\varprojlim_m H_{\text{unr}}^1(D_{m,\mathfrak{l}}, E[p^k]) \cong \Lambda/p^k\Lambda$$

taking $\text{loc}_{\mathfrak{l}}(\kappa_{\mathfrak{n}})$ to $\lambda_{\mathfrak{n}\mathfrak{l}}$.

Since the empty product lies in \mathfrak{N}_k for every k , we obtain a distinguished element

$$(6) \quad \begin{aligned} \lambda^\infty \in \Lambda & \quad \text{if } \epsilon(N^-) = -1 \\ \kappa^\infty \in \mathcal{S} & \quad \text{if } \epsilon(N^-) = 1 \end{aligned}$$

defined as the inverse limit of λ_1 or κ_1 as k varies.

Lemma 3.2.2. *The Λ -module \mathcal{S} is torsion free.*

Proof. As the torsion subgroup of $E(D_\infty)$ is finite (since D_∞ has primes of finite residue degree), $H^0(D_\infty, T_p(E)) = 0$ and the claim follows from [11, Lemma 1.3.3]. \square

The following theorem will be proved in §3.4.

Theorem 3.2.3. *Assume that the special element (6) is nonzero and let $X_{\Lambda-\text{tors}}$ denote the torsion submodule of X .*

(a) *One has the rank formulas*

$$\text{rank}_\Lambda \mathcal{S} = \text{rank}_\Lambda X = \begin{cases} 0 & \text{if } \epsilon(N^-) = -1 \\ 1 & \text{if } \epsilon(N^-) = 1. \end{cases}$$

(b) *For any height one prime \mathfrak{P} of Λ one has*

$$\text{ord}_{\mathfrak{P}}(\text{char}(X_{\Lambda-\text{tors}})) \leq 2 \cdot \begin{cases} \text{ord}_{\mathfrak{P}}(\lambda^\infty) & \text{if } \epsilon(N^-) = -1 \\ \text{ord}_{\mathfrak{P}}(\text{char}(\mathcal{S}/\Lambda\kappa^\infty)) & \text{if } \epsilon(N^-) = 1. \end{cases}$$

(c) *Equality holds in (b) if the following condition is satisfied: there exists a k_0 such that for all $j \geq k_0$ the set*

$$\{\lambda_{\mathfrak{n}} \in \Lambda/p^j \Lambda \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{definite}}\}$$

contains an element with nontrivial image in $\Lambda/(\mathfrak{P}, p^{k_0})$.

3.3. Reduction at a height one prime. Set $V_p(E) = T_p(E) \otimes \mathbf{Q}_p$, so that we have the exact sequence

$$(7) \quad 0 \rightarrow T_p(E) \rightarrow V_p(E) \rightarrow E[p^\infty] \rightarrow 0.$$

Fix $\mathfrak{P} \neq p\Lambda$ a height-one prime of Λ , and denote by $\mathcal{O}_{\mathfrak{P}}$ the integral closure of Λ/\mathfrak{P} , viewed as a Galois module with trivial action. The ring $\mathcal{O}_{\mathfrak{P}}$ is the ring of integers of a finite extension $\Phi_{\mathfrak{P}}/\mathbf{Q}_p$, and we denote by $\mathfrak{m}_{\mathfrak{P}}$ its maximal ideal. By tensoring (7) with $\mathcal{O}_{\mathfrak{P}}$ (viewed as a G_K -module via the natural map $G_K \rightarrow \Lambda^\times$), we obtain an exact sequence of $\mathcal{O}_{\mathfrak{P}}[[G_K]]$ -modules

$$(8) \quad 0 \rightarrow T_{\mathfrak{P}} \rightarrow V_{\mathfrak{P}} \rightarrow W_{\mathfrak{P}} \rightarrow 0.$$

For any prime \mathfrak{q} of K and A and one of $T_{\mathfrak{P}}$, $V_{\mathfrak{P}}$, or $W_{\mathfrak{P}}$, we define a submodule

$$H_{\mathcal{F}_{\mathfrak{P}}}^1(K_{\mathfrak{q}}, M) \subset H^1(K_{\mathfrak{q}}, M)$$

as follows. First suppose $M = V_{\mathfrak{P}}$. If $\mathfrak{q} \nmid pN^-$ then $H_{\mathcal{F}_{\mathfrak{P}}}^1(K_{\mathfrak{q}}, V_{\mathfrak{P}})$ is the unramified cohomology classes. If $\mathfrak{q} \mid pN^-$ then $H_{\mathcal{F}_{\mathfrak{P}}}^1(K_{\mathfrak{q}}, V_{\mathfrak{P}})$ is defined to be the image of

$$H^1(K_{\mathfrak{q}}, \text{Fil}_{\mathfrak{q}}(T_p(E)) \otimes \Phi_{\mathfrak{P}}) \rightarrow H^1(K_{\mathfrak{q}}, V_{\mathfrak{P}}).$$

If $M = T_{\mathfrak{P}}$ or $W_{\mathfrak{P}}$, then $H_{\mathcal{F}_{\mathfrak{P}}}^1(K_{\mathfrak{q}}, M)$ is obtained from $H_{\mathcal{F}_{\mathfrak{P}}}^1(K_{\mathfrak{q}}, V_{\mathfrak{P}})$ by propagation, in the sense of Remark 2.1.3. These local submodules define global Selmer groups which we denote by $\text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, M)$.

Proposition 3.3.1. *Shapiro's lemma, the natural map $T_p(E) \otimes \Lambda \rightarrow T_{\mathfrak{P}}$, and its dual induce maps*

$$\mathcal{S}/\mathfrak{P}\mathcal{S} \rightarrow \text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}}) \quad \text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}}) \rightarrow \text{Sel}(D_\infty, E[p^\infty])[\mathfrak{P}].$$

The first map is injective. There is a finite set of height one primes Σ_Λ of Λ such that if $\mathfrak{P} \notin \Sigma_\Lambda$, then these maps have finite kernel and cokernel which are bounded by a constant depending on $[\mathcal{O}_{\mathfrak{P}} : \Lambda/\mathfrak{P}]$ but not on \mathfrak{P} itself.

Proof. The proof requires only minor modifications from that of [10, Proposition 5.3.14]. One must first prove a local control theorem at each prime \mathfrak{q} of K . If $\mathfrak{q} \nmid pN^-$ this local result is [10, Lemma 5.3.13]. If $\mathfrak{q} \mid p$ the desired result is [8, Lemma 2.2.7]. The case $\mathfrak{q} \mid N^-$ is similar to the latter, but is greatly simplified by the fact that such \mathfrak{q} split completely in D_∞ . With the local control results in hand, the remainder of the proof follows that of [10, Proposition 5.3.14] verbatim. \square

Lemma 3.3.2. *Abbreviate $\mathcal{S}_{\mathfrak{P}} = \text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}})$. The natural map*

$$\mathcal{S}_{\mathfrak{P}}/p^k \mathcal{S}_{\mathfrak{P}} \rightarrow \text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}}/p^k T_{\mathfrak{P}})$$

is injective, where the Selmer structure on $T_{\mathfrak{P}}/p^k T_{\mathfrak{P}}$ is obtained from the Selmer structure on $T_{\mathfrak{P}}$ by propagation (Remark 2.1.3).

Proof. This is Lemma 3.7.1 of [10]. \square

For any pair of positive integers $k \leq j$, set

$$\delta_{\mathfrak{P}}(k, j) = \min\{\text{ind}(\lambda_{\mathfrak{n}}, \mathcal{O}_{\mathfrak{P}}/p^k \mathcal{O}_{\mathfrak{P}}) \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{definite}}\} \leq \infty.$$

As $\delta_{\mathfrak{P}}(k, j) \leq \delta_{\mathfrak{P}}(k, j+1)$, we may define $\delta_{\mathfrak{P}}(k) = \lim_{j \rightarrow \infty} \delta_{\mathfrak{P}}(k, j)$.

Proposition 3.3.3. *If $\epsilon(N^-) = -1$ and $\lambda^\infty \in \Lambda$ has nontrivial image in $\mathcal{O}_{\mathfrak{P}}/p^k \mathcal{O}_{\mathfrak{P}}$ then*

$$\text{length}_{\mathcal{O}_{\mathfrak{P}}}(\text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}})) + 2\delta_{\mathfrak{P}}(k) = 2 \cdot \text{length}_{\mathcal{O}_{\mathfrak{P}}}(\mathcal{O}_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}\lambda^\infty).$$

If $\epsilon(N^-) = 1$ and κ^∞ has nontrivial image in $\mathcal{S}_{\mathfrak{P}}/p^k \mathcal{S}_{\mathfrak{P}}$ then

- (a) $\mathcal{S}_{\mathfrak{P}}$ is free of rank one over $\mathcal{O}_{\mathfrak{P}}$,
- (b) $\text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}})$ has $\mathcal{O}_{\mathfrak{P}}$ -corank one, and
- (c) $\text{length}_{\mathcal{O}_{\mathfrak{P}}}(\text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}})_{/\text{div}}) + 2\delta_{\mathfrak{P}}(k) = 2 \cdot \text{length}_{\mathcal{O}_{\mathfrak{P}}}(\mathcal{S}_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}\kappa^\infty)$ (the sub-script $/\text{div}$ indicates the quotient by the maximal $\mathcal{O}_{\mathfrak{P}}$ -divisible submodule).

Proof. Let k be as in the statement of the proposition. For any $j \geq k$, abbreviate

$$T_j = T_{\mathfrak{P}}/p^j T_{\mathfrak{P}} \quad R_j = \mathcal{O}_{\mathfrak{P}}/p^j \mathcal{O}_{\mathfrak{P}}.$$

Let \mathcal{F} denote the Selmer structure on T_j obtained by propagation (Remark 2.1.3) of $\mathcal{F}_{\mathfrak{P}}$ from $T_{\mathfrak{P}}$, and use the same notation for the Selmer structure on $W_{\mathfrak{P}}[p^j]$ propagated from $\mathcal{F}_{\mathfrak{P}}$ on $W_{\mathfrak{P}}$. By applying the reduction maps $\Lambda/p^j \rightarrow R_j$ and

$$\varprojlim_m H^1(D_m, E[p^j]) \cong H^1(K, E[p^j] \otimes \Lambda) \rightarrow H^1(K, T_j)$$

to the Euler system (5), we obtain families

$$(9) \quad \{\bar{\kappa}_{\mathfrak{n}} \in \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_j) \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{indefinite}}\} \quad \{\bar{\lambda}_{\mathfrak{n}} \in R_j \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{definite}}\}$$

By assumption (and Lemma 3.3.2), $\bar{\kappa}_1$ or $\bar{\lambda}_1$ (depending on whether $\epsilon(N^-) = 1$ or -1) is nontrivial, where $1 \in \mathfrak{N}_j$ is the empty product.

A choice of uniformizer of $\mathcal{O}_{\mathfrak{P}}$ determines an isomorphism $T_j \cong W_{\mathfrak{P}}[p^j]$, and under such an isomorphism the Selmer structures \mathcal{F} are identified (as in the proof of Lemma 1.3.8(i) of [12]). In particular

$$(10) \quad \text{Sel}_{\mathcal{F}}(K, T_j) \cong \text{Sel}_{\mathcal{F}}(K, W_{\mathfrak{P}}[p^j]) \cong \text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}})[p^j],$$

where the second isomorphism follows from Lemma 2.2.6 and the following

Lemma 3.3.4. *The triple $(T_j, \mathcal{F}, \mathfrak{L}_j)$ satisfies Hypotheses 2.2.4 and 2.3.1, as well as the hypotheses of §2.6. More precisely the following hold.*

- (a) T_j is residually an absolutely irreducible G_K -module.
- (b) For any $\mathfrak{l} \in \mathfrak{L}_j$, the Frobenius at \mathfrak{l} acts on T_j with eigenvalues $\mathbf{N}(\mathfrak{l})$ and 1.
- (c) There is a perfect R_j -bilinear symmetric pairing $T_j \times T_j \rightarrow R_j(1)$ satisfying $(s^\sigma, t^{\tau\sigma}) = (s, t)^\sigma$ for any $\sigma \in G_K$.
- (d) The Selmer structure \mathcal{F} is cartesian in the sense of Definition 2.2.2, and is self-dual in the sense of §2.6, relative to the pairing above.
- (e) The set \mathfrak{L}_j satisfies Hypothesis 2.3.1.

Proof. Since \mathfrak{l} splits completely in D_∞ , there is an isomorphism of Galois modules $T_{\mathfrak{p}} \cong T_p(E) \otimes \mathcal{O}_{\mathfrak{p}}$ with $G_{K_{\mathfrak{l}}}$ acting *trivially* on $\mathcal{O}_{\mathfrak{p}}$. In particular, the residual representation of $T_{\mathfrak{p}}$ is absolutely irreducible since $E[p]$ is (by Hypothesis 3.0.1), and property (b) is immediate from the definition of a k -admissible prime. Define an $\mathcal{O}_{\mathfrak{p}}(1)$ -valued pairing on $T_{\mathfrak{p}}$ by the rule

$$(x \otimes \alpha, y \otimes \beta)_{\mathfrak{p}} = \alpha\beta \cdot (x, y^\tau),$$

where (\cdot, \cdot) is the Weil pairing on $T_p(E)$. The reduction of this pairing modulo p^j defines the pairing of (c). The cartesian property of (d) is a consequence of the fact that the Selmer structure $\mathcal{F}_{\mathfrak{p}}$ on $T_{\mathfrak{p}}$ is obtained by propagation from $V_{\mathfrak{p}}$; see [10, Lemma 3.7.1]. The self-duality follows from this and the self-duality of the local conditions defining the canonical Selmer structure on $V_{\mathfrak{p}}$. Part (e) is [2, Theorem 3.2]. \square

Lemma 3.3.5. *The decomposition $\mathfrak{N}_j = \mathfrak{N}_j^{\text{odd}} \sqcup \mathfrak{N}_j^{\text{even}}$ (relative to the data $T, \mathcal{F}, \mathfrak{L}_j$) of Definition 2.2.8 is given by*

$$(11) \quad \mathfrak{N}_j^{\text{odd}} = \mathfrak{N}_j^{\text{indefinite}} \quad \mathfrak{N}_j^{\text{even}} = \mathfrak{N}_j^{\text{definite}}.$$

Furthermore, the families (9) form an Euler system of odd type for $(T_j, \mathcal{F}, \mathfrak{L}_j)$.

Proof. First note that either (11) holds or the opposite relation

$$\mathfrak{N}_j^{\text{even}} = \mathfrak{N}_j^{\text{indefinite}} \quad \mathfrak{N}_j^{\text{odd}} = \mathfrak{N}_j^{\text{definite}}$$

holds (simply because the even/odd decomposition of \mathfrak{N}_j is determined by the function $\rho(\mathfrak{n})$ of Corollary 2.2.10, the definite/indefinite decomposition is determined by $\epsilon(\mathfrak{n})$, and both functions are multiplied by -1 when one replaces \mathfrak{n} by $\mathfrak{n}\mathfrak{l}$.) The reciprocity laws of §3.2 imply that the reduced families (9) satisfy the reciprocity laws of Definition 2.3.2, and so this family forms a nonzero Euler system which is of odd type if (11) holds, and is of even type otherwise. By Proposition 2.3.4, the Euler system must be of odd type, so (11) holds. \square

The Euler system of the lemma for $(T_k, \mathcal{F}, \mathfrak{L}_k)$ may not be free, but this can be remedied by shrinking the set of indexing primes \mathfrak{L}_k slightly.

Lemma 3.3.6. *For any $j \geq 2k$ the families*

$$\{\bar{\kappa}_{\mathfrak{n}} \in \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_k) \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{indefinite}}\} \quad \{\bar{\lambda}_{\mathfrak{n}} \in R_k \mid \mathfrak{n} \in \mathfrak{N}_j^{\text{definite}}\}$$

form a free Euler system of odd type for $(T_k, \mathcal{F}, \mathfrak{L}_j)$.

Proof. Fix $\mathfrak{n} \in \mathfrak{N}_j^{\text{odd}} = \mathfrak{N}_j^{\text{indefinite}}$ and $j \geq 2k$. We must show that there is a free rank one R_k -submodule of $\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_k)$ containing $\bar{\kappa}_{\mathfrak{n}}$. By Proposition 2.2.7 we may decompose

$$\text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_j) \cong R_j \oplus N \oplus N \quad \text{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_k) \cong R_k \oplus M \oplus M.$$

Let \mathfrak{m} be the maximal ideal of $\mathcal{O}_{\mathfrak{p}}$ and fix a uniformizer π . Let e be the ramification degree of $\mathcal{O}_{\mathfrak{p}}$, so that R_k has length ek . If $\mathfrak{m}^{ek-1}M \neq 0$ then $\bar{\kappa}_{\mathfrak{n}} = 0$ by Proposition 2.3.5, and there is nothing to prove. Assume therefore that $\mathfrak{m}^{ek-1}M = 0$. Lemma

2.2.6 gives a commutative diagram

$$\begin{array}{ccc} \mathrm{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_j) & \xrightarrow{\pi^{e(j-k)}} & \mathrm{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_j)[\mathfrak{m}^{ek}] \\ \downarrow & \nearrow \cong & \\ \mathrm{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_k) & & \end{array}$$

The diagonal isomorphism implies that $\mathfrak{m}^{ek-1} \cdot \mathrm{Sel}_{\mathcal{F}(\mathfrak{n})}(K, T_j)[\mathfrak{m}^{ek}]$ is a cyclic module, and so $\mathfrak{m}^{ek-1}N = 0$. But $j \geq 2k$ then implies that the image of N under the vertical arrow is zero, and hence the image of the vertical arrow is free of rank one. Since $\bar{\kappa}_{\mathfrak{n}}$ is contained in this image, the claim is proved. \square

Now fix $j \geq 2k$. Since $\mathfrak{N}_j^{\mathrm{even}} = \mathfrak{N}_j^{\mathrm{definite}}$, the empty product lies in $\mathfrak{N}_j^{\mathrm{even}}$ if and only if $\epsilon(N^-) = -1$. If this is the case, then applying Theorem 2.5.1 with $\mathfrak{n} = 1$ tells us that $\mathrm{Sel}_{\mathcal{F}}(K, T_k) \cong M \oplus M$ with

$$\mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(M) + \delta_{\mathfrak{p}}(k, j) = \mathrm{ind}(\bar{\lambda}_1, R_k) = \mathrm{ind}(\lambda^\infty, \mathcal{O}_{\mathfrak{p}}/p^k \mathcal{O}_{\mathfrak{p}}).$$

In particular, since the right hand side is $< k$, (10) implies that $M \oplus M \cong \mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, W_{\mathfrak{p}})$. We conclude

$$\mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(\mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, W_{\mathfrak{p}})) + 2 \cdot \delta_{\mathfrak{p}}(k, j) = 2 \cdot \mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}\lambda^\infty).$$

Now consider the case $\epsilon(N^-) = 1$. First note that Theorem 2.5.1 (again with $\mathfrak{n} = 1$) tells us that $\mathrm{Sel}_{\mathcal{F}}(K, T_k) \cong R \oplus M \oplus M$ with

$$\mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(M) + \delta_{\mathfrak{p}}(k, j) = \mathrm{ind}(\bar{\kappa}_1, \mathrm{Sel}_{\mathcal{F}}(K, T_k)).$$

As above, this implies that $\mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(M) < k$. Combining this with (10) tells us that $\mathcal{S}_{\mathfrak{p}} \cong \varprojlim_k \mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, W_{\mathfrak{p}})[p^k]$ is a torsion-free rank-one $\mathcal{O}_{\mathfrak{p}}$ -module. By [10, Lemma 3.7.1] the reduction map

$$\mathcal{S}_{\mathfrak{p}}/p^k \mathcal{S}_{\mathfrak{p}} \rightarrow \mathrm{Sel}_{\mathcal{F}}(K, T_k)$$

is injective, and it follows from Theorem 2.5.1 that

$$\begin{aligned} \mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(\mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, W_{\mathfrak{p}})_{/\mathrm{div}}) + 2\delta_{\mathfrak{p}}(k, j) &= \mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(M \oplus M) + 2\delta_{\mathfrak{p}}(k, j) \\ &= 2 \cdot \mathrm{ind}(\bar{\kappa}_1, \mathrm{Sel}_{\mathcal{F}}(K, T_k)) \\ &= 2 \cdot \mathrm{length}_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{S}_{\mathfrak{p}}/\mathcal{S}_{\mathfrak{p}}\kappa^\infty). \end{aligned}$$

Now take $j \rightarrow \infty$. This completes the proof of Proposition 3.3.3. \square

3.4. Proof of Theorem 3.2.3. The theorem is reduced to Proposition 3.3.3 exactly as in the proof of Theorem 5.3.10 of [10].

Assume that κ^∞ or λ^∞ is nonzero, depending on whether we are in the case $\epsilon(N^-) = 1$ or -1 . Since \mathcal{S} is a finitely generated torsion-free Λ -module (Lemma 3.2.2), if $\epsilon(N^-) = 1$ it is easily seen that the image of κ^∞ in $\mathcal{S}/\mathfrak{p}\mathcal{S}$ is nonzero for all but finitely many height-one primes \mathfrak{p} . Similar comments hold for λ^∞ when $\epsilon(N^-) = -1$. Fix a finite set Σ_Λ of height one primes of Λ as in Proposition 3.3.1 large enough that Σ_Λ contains $p\Lambda$ and all prime divisors of the characteristic ideal of the torsion submodule of X , and large enough that the special element (6) has nonzero image in $\mathcal{S}/\mathfrak{p}\mathcal{S}$ or $\Lambda/\mathfrak{p}\Lambda$ for all $\mathfrak{p} \notin \Sigma_\Lambda$.

Fix any $\mathfrak{p} \notin \Sigma_\Lambda$ and suppose $\epsilon(N^-) = 1$. By Proposition 3.3.1, κ^∞ has nonzero image in $\mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, T_{\mathfrak{p}})$. Proposition 3.3.3 then implies that $\mathrm{Sel}_{\mathcal{F}_{\mathfrak{p}}}(K, T_{\mathfrak{p}})$ and

$\text{Sel}_{\mathcal{F}_{\mathfrak{P}}}(K, W_{\mathfrak{P}})$ have rank and corank one (respectively) as $\mathcal{O}_{\mathfrak{P}}$ -modules. It now follows from Proposition 3.3.1 that

$$\text{rank}_{\Lambda} \mathcal{S} = \text{rank}_{\mathcal{O}_{\mathfrak{P}}}(\mathcal{S} \otimes_{\Lambda} \mathcal{O}_{\mathfrak{P}}) = 1$$

and similarly for X . The case $\epsilon(N^-) = -1$ is similar, and this completes the proof of (a).

Let \mathfrak{P} be any height-one prime of Λ different from $p\Lambda$, and let $f \in \Lambda$ be a distinguished polynomial which generates \mathfrak{P} . For each positive integer m set $\mathfrak{P}_m = (f + p^m)\Lambda$. For $m \gg 0$, \mathfrak{P}_m is a prime ideal $\notin \Sigma_{\Lambda}$ with $\Lambda/\mathfrak{P} \cong \Lambda/\mathfrak{P}_m$ as rings (by Hensel's lemma). Arguing as in the proof of Theorem 5.3.10 of [10] and using Proposition 3.3.1, we obtain

$$\text{length}_{\mathbf{Z}_p}(\text{Sel}_{\mathcal{F}_{\mathfrak{P}_m}}(K, W_{\mathfrak{P}_m})_{/\text{div}}) = m \text{rank}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{P}}) \cdot \text{ord}_{\mathfrak{P}}(\text{char}(X_{\Lambda-\text{tors}}))$$

up to $O(1)$ as m varies. Similarly, writing $\mathcal{S}_{\mathfrak{P}_m} = \text{Sel}_{\mathcal{F}_{\mathfrak{P}_m}}(K, T_{\mathfrak{P}_m})$,

$$\begin{aligned} \text{length}_{\mathbf{Z}_p}(\mathcal{S}_{\mathfrak{P}_m}/\mathcal{O}_{\mathfrak{P}_m}\kappa^{\infty}) &= m \text{rank}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{P}}) \cdot \text{ord}_{\mathfrak{P}}(\text{char}(\mathcal{S}/\Lambda\kappa^{\infty})) \\ \text{length}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{P}_m}/\mathcal{O}_{\mathfrak{P}_m}\lambda^{\infty}) &= m \text{rank}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{P}}) \cdot \text{ord}_{\mathfrak{P}}(\lambda^{\infty}) \end{aligned}$$

when $\epsilon(N^-) = 1$ or -1 , respectively, up to $O(1)$ as m varies. Proposition 3.3.3 (with $k \gg 0$) gives the inequality

$$\begin{aligned} \text{length}_{\mathbf{Z}_p}(\text{Sel}_{\mathcal{F}_{\mathfrak{P}_m}}(K, W_{\mathfrak{P}_m})_{/\text{div}}) + 2e\delta_{\mathfrak{P}_m}(k) &= 2 \cdot \text{length}_{\mathbf{Z}_p}(\mathcal{S}_{\mathfrak{P}_m}/\mathcal{O}_{\mathfrak{P}_m}\kappa^{\infty}) \\ \text{length}_{\mathbf{Z}_p}(\text{Sel}_{\mathcal{F}_{\mathfrak{P}_m}}(K, W_{\mathfrak{P}_m})) + 2e\delta_{\mathfrak{P}_m}(k) &= 2 \cdot \text{length}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{P}_m}/\mathcal{O}_{\mathfrak{P}_m}\lambda^{\infty}) \end{aligned}$$

(again, when $\epsilon(N^-) = 1$ or -1 , respectively) where e is the absolute ramification degree of $\mathcal{O}_{\mathfrak{P}_m}$, which is independent of m . As $\delta_{\mathfrak{P}_m}(k) \geq 0$, letting $m \rightarrow \infty$ proves the inequality of (b) when $\mathfrak{P} \neq p\Lambda$.

We show that under the additional hypothesis of (c) the value of $\delta_{\mathfrak{P}_m}(k)$ is bounded as m and k vary. For every $j \geq k_0$ let $\mathbf{n}(j) \in \mathfrak{N}_j^{\text{definite}}$ be such that $\lambda_{\mathbf{n}(j)}$ has nonzero image in $\Lambda/(\mathfrak{P}, p^{k_0})$. Then $\lambda_{\mathbf{n}(j)}$ has nontrivial image in $\Lambda/(\mathfrak{P}_m, p^{k_0})$ for all $m \geq k_0$. Define C_m to be the cokernel of $\Lambda/\mathfrak{P}_m \hookrightarrow \mathcal{O}_{\mathfrak{P}_m}$. The groups C_m are finite, and up to isomorphism do not depend on m . If k_1 is large enough that $p^{k_1-k_0}$ kills C_m , then we have the exact and commutative diagram

$$\begin{array}{ccccc} C_m[p^{k_1}] & \longrightarrow & \Lambda/(\mathfrak{P}_m, p^{k_1}) & \longrightarrow & \mathcal{O}_{\mathfrak{P}_m}/p^{k_1}\mathcal{O}_{\mathfrak{P}_m} \\ \downarrow 0 & & \downarrow & & \downarrow \\ C_m[p^{k_0}] & \longrightarrow & \Lambda/(\mathfrak{P}_m, p^{k_0}) & \longrightarrow & \mathcal{O}_{\mathfrak{P}_m}/p^{k_0}\mathcal{O}_{\mathfrak{P}_m}. \end{array}$$

It follows that $\lambda_{\mathbf{n}(j)}$ has nontrivial image in $\mathcal{O}_{\mathfrak{P}_m}/p^{k_1}\mathcal{O}_{\mathfrak{P}_m}$ for all $j \geq k_1$. For $j \geq k \geq k_1$ we then have

$$\delta_{\mathfrak{P}_m}(k, j) \leq \text{ind}(\lambda_{\mathbf{n}(j)}, \mathcal{O}_{\mathfrak{P}_m}/p^k\mathcal{O}_{\mathfrak{P}_m}) < ek_1,$$

hence $\delta_{\mathfrak{P}_m}(k) < ek_1$ for all $k \geq k_1$ and any $m \geq k_0$.

Finally, if $\mathfrak{P} = p\Lambda$, one instead takes $\mathfrak{P}_m = ((\gamma - 1)^m + p)\Lambda$ for some generator $\gamma \in \Gamma$ and a similar argument holds. This completes the proof of Theorem 3.2.3.

REFERENCES

- [1] M. Bertolini. Selmer groups and Heegner points in anticyclotomic \mathbf{Z}_p -extensions. *Compositio Math.*, 99(2):153–182, 1995.
- [2] M. Bertolini and H. Darmon. Iwasawa’s Main Conjecture for elliptic curves over anticyclotomic \mathbf{Z}_p -extensions. To appear in *Ann. of Math.*
- [3] M. Bertolini and H. Darmon. Euler systems and Jochnowitz congruences. *Amer. J. Math.*, 121(2):259–281, 1999.
- [4] C. Cornut. Mazur’s conjecture on higher Heegner points. *Invent. Math.*, 148(3):495–523, 2002.
- [5] H Darmon and A Iovita. The anticyclotomic main conjecture for supersingular elliptic curves. Preprint.
- [6] B. Gross. Heights and the special values of L -series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.
- [7] B.. Gross and S. Kudla. Heights and the central critical values of triple product L -functions. *Compositio Math.*, 81(2):143–209, 1992.
- [8] B. Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.
- [9] B. Howard. Iwasawa theory of Heegner points on abelian varieties of GL_2 type. *Duke Math. J.*, 124(1):1–45, 2004.
- [10] B. Mazur and K. Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.
- [11] B. Perrin-Riou. *p -adic L -functions and p -adic Representations*. American Mathematical Society, 1995.
- [12] K. Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA.

Current address: Department of Mathematics, University of Chicago, 5734 S. University Ave., Chicago, IL 60637

E-mail address: howard@math.uchicago.edu